CLAIMS

1. A method for providing content identification within a media data stream comprising the steps of:

receiving a data stream of media content;

inserting content identification data at regular intervals within the media data stream.

2. The method of claim 1 wherein the content identification data is inserted every frame.

3. The method of claim 1 wherein the content identification data is digitally combined with a predetermined property of the data stream.

4. The method of claim 1 for providing tamper resistant content identification within the media data stream, in which the step of inserting content identification data comprises the further steps of:

extracting data relating to a predetermined property of the media data stream;

combining the extracted data with content identification data;

applying a digital signature to the combined data; and

inserting the combined data and digital signature as secured content identification data into the data stream.

5. The method of claim 4 in which the step of combining the extracted data with content identification data comprises the step of forming a hash code from the extracted data and the content identification data.

6. The method of claim 1 in which the media data stream may comprise any one or more of pictures and audio or video data streams.

7. The method of claim 3 in which the predetermined property is any property of the media data stream that changes from data frame to data frame.

8. The method of claim 7 in which the predetermined property comprises any one or more of: frame size, frame hash, transport stream identifier, clock signal, and continuity count.

9. The method of claim 8 in which the predetermined property is a combination of frame size and frame hash.

10. The method of claim 5 in which the step of applying a digital signature to the hash code further includes applying digital signatures of the originator of the media data stream and a certification authority.

11. A method of transcoding a media data stream comprising the steps of:

receiving a data stream of media content including embedded, secured content identification data, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream;

transcoding the media content of the data stream into a new format;

extracting data relating to a predetermined property of the media data stream in its new format;

extracting content identification data from the secured content identification data;

combining the extracted data with the extracted content identification data;

applying a digital signature to the combined data; and

inserting the combined data and digital signature as re-secured content identification data into the data stream.

12. The method of claim 11 in which the new format of the data stream has a lower resolution or transmission / storage bandwidth than the original format of the data stream.

13. The method of claim 11 in which the media content may comprise any one or more of pictures, audio, video data streams.

14. The method of claim 11 in which the predetermined property is any property of the media data stream that changes from data frame to data frame.

15. The method of claim 14 in which the predetermined property comprises any one or more of: frame size, frame hash, transport stream identifier, clock signal, and continuity count.

16. The method of claim 15 in which the predetermined property is a combination of frame size and frame hash.

17. The method of claim 11 in which the step of applying a digital signature to the combined data further includes applying a digital signature of the transcoding device.

18. The method of claim 17 in which the step of applying a digital signature to the combined data further includes the step of making available a corresponding public key of the transcoding device that is digitally signed by the originator of the content identification data.

19. The method of claim 11 in which the step of combining the extracted data with the extracted content identification data further includes the step of modifying the extracted content identification data.

20. The method of claim 19 in which the step of modifying the extracted content identification data comprises including an indication of the new format of the transcoded data stream.

21. The method of claim 19 in which the step of modifying the extracted content identification data comprises including an identity of a device performing the transcoding.

22. A method of verifying the integrity of secured content identification data embedded in a media data stream, comprising the steps of:

receiving a data stream of media content including embedded, secured content identification data, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream;

extracting first data relating to a predetermined property of the media data stream;

extracting content identification data from the secured content identification data;

extracting second data relating to the predetermined property from the secured content identification data;

comparing the first data and the second data to verify the authenticity of the extracted content identification data.

23. The method of claim 22 in which the step of extracting content identification data from the secured content identification data comprises the steps of:

obtaining a public key of a content provider that secured the content identification data; and

verifying an encrypted signature of the content provider using the public key.

24. The method of claim 23 in which the step of extracting content identification data from the secured content identification data comprises the steps of:

obtaining a public key of a certification authority;

verifying the authenticity of the public key of the content provider using the public key of the certification authority.

25. The method of claim 22 in which the media data stream is received via a transcoding device, and in which the step of extracting content identification data from the secured content identification data comprises the steps of verifying that the transcoder device was authorised to modify the data stream by an originator of the content identification data.

26. The method of claim 25 in which the step of extracting content identification data from the secured content identification data comprises the steps of:

obtaining a public key of the transcoding device that secured the content identification data, the public key being digitally signed by the originator of the content identification data;

obtaining a public key of the originator;

verifying an encrypted signature of the originator using the public key of the originator, and thereby verifying the public key of the transcoder device;

verifying the content identification information using the verified public key of the transcoder device.

27. The method of claim 22 in which the media content may comprise any one or more of pictures, audio, video data streams.

28. The method of claim 22 in which the predetermined property is any property of the media data stream that changes from data frame to data frame.

29. The method of claim 28 in which the predetermined property comprises any one or more of: frame size, frame hash, transport stream identifier, clock signal, and continuity count.

30. The method of claim 29 in which the predetermined property is a combination of frame size and frame hash.

31. Apparatus for providing content identification within a media data stream comprising:

means for receiving a data stream of media content;

means for inserting content identification data at regular intervals within the media data stream.

32. The apparatus of claim 31 wherein the means for inserting comprises:

a data extraction module for extracting data relating to a predetermined property of the media data stream;

means for combining the extracted data with content identification data;

an encryption module for applying a digital signature to the combined data; and

a data merge module for inserting the combined data and digital signature as secured content identification data into the data stream.

33. The apparatus of claim 32 in which the means for combining includes a hash function generator for forming a hash code from the combined data, the encryption module applying the digital signature to the hash code.

34. Apparatus for transcoding a media data stream, comprising:

means for receiving a data stream of media content including embedded, secured content identification data, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream;

a transcoder module for transcoding the media content of the data stream into a new format;

a data extraction module for extracting data relating to a predetermined property of the media data stream in its new format and for extracting content identification data from the secured content identification data;

means for combining the extracted data with the extracted content identification data;

an encryption module for applying a digital signature to the combined data; and

a data merge module for inserting the combined data and digital signature as re-secured content identification data into the data stream.

35. Apparatus for verifying the integrity of secured content identification data embedded in a media data stream, comprising:

means for receiving a data stream of media content including embedded, secured content identification data, in which the secured content identification data incorporates data relating to a predetermined property of the media data stream;

a data extraction module for extracting first data relating to a predetermined property of the media data stream;

a decryption module for extracting content identification data from the secured content identification data; and for extracting second data relating to the predetermined property from the secured content identification data;

a compare module for comparing the first data and the second data to verify the authenticity of the extracted content identification data.

36. A computer program product, comprising a computer readable medium having thereon computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the procedure of any one of claims 1 to 30.

37. A computer program product, distributable by electronic data transmission, comprising computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the procedure of any one of claims 1 to 30.